ABSTRACT OF THE DISCLOSURE

A system and method is provided for automatically identifying and removing malicious data packets, such as denial-of-service (DoS) packets, in an intermediate network node before the packets can be forwarded to a central processing unit (CPU) in the node. The CPU's processing bandwidth is therefore not consumed identifying and removing the malicious packets from the system memory. As such, processing of the malicious packets is essentially "off-loaded" from the CPU, thereby enabling the CPU to process non-malicious packets in a more efficient manner. Unlike prior implementations, the invention identifies malicious packets having complex encapsulations that can not be identified using traditional techniques, such as ternary content addressable memories (TCAM) or lookup tables.